



QUALYS SECURITY CONFERENCE 2018

Real-Time Vulnerability Management

Operationalizing the VM process from detection to remediation

Michael Kassim,
Account Manager, Qualys, Inc.

Giorgio Gheri
Security Solutions Architect, Qualys, Inc.

Agenda

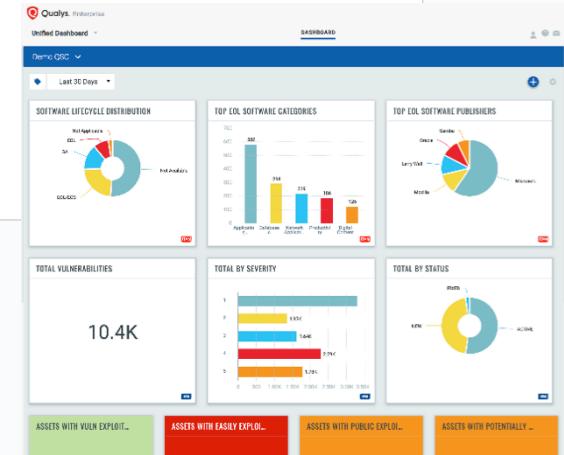
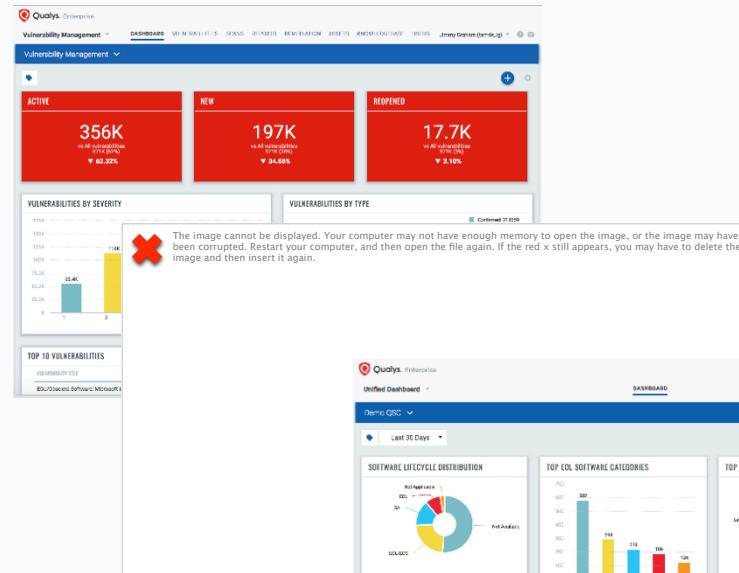
Expanding Vulnerability Management

Unified Dashboard

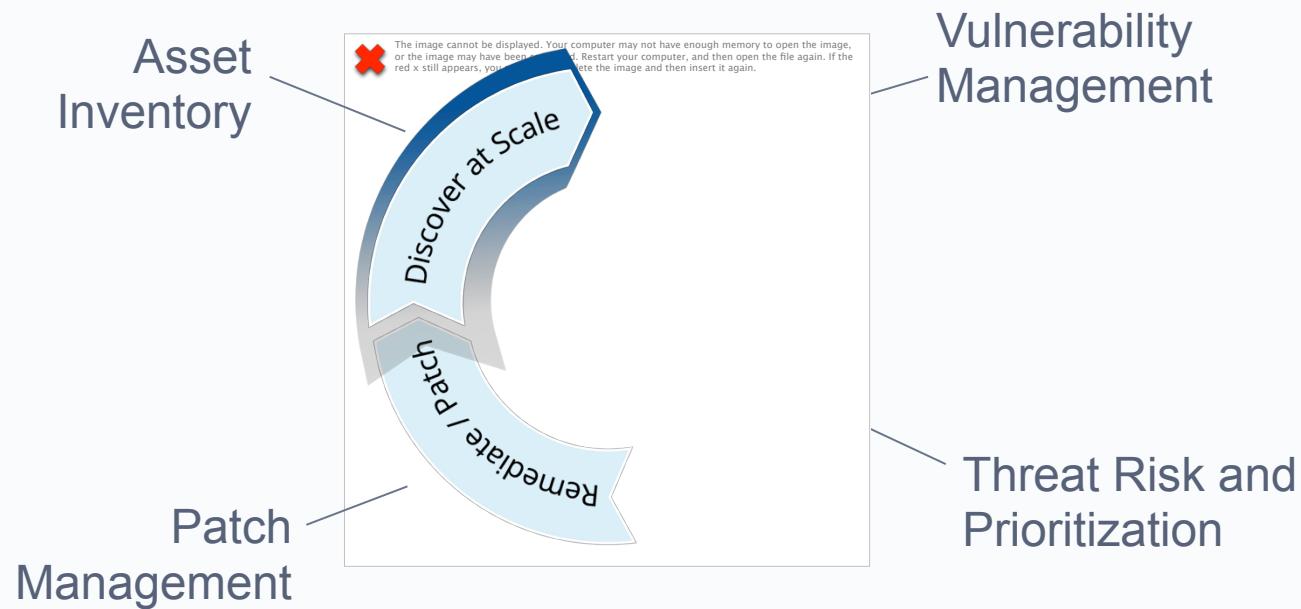
Introducing Qualys Patch Management

QSC
2 Conference,
2010

04
Decemb
er 2010



Vulnerability Management Lifecycle



Expanding Vulnerability Management





Vulnerability Management

Platform Evolution

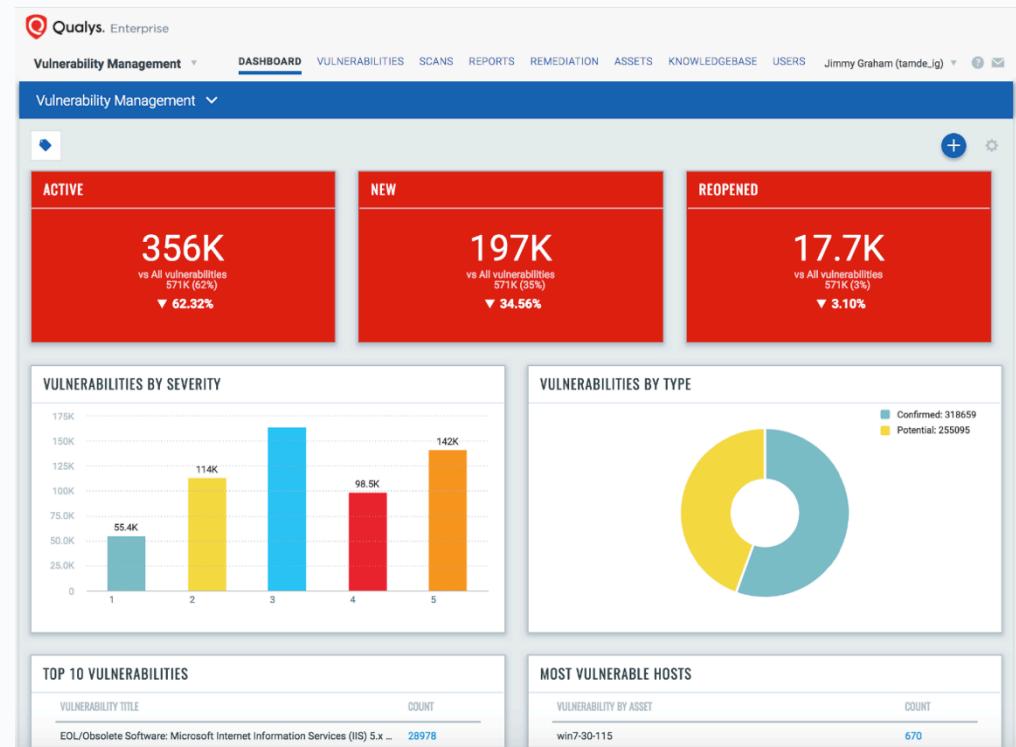
Elastic VM Dashboard

Merges AssetView
technology into Qualys VM

Build widgets with
vulnerability counts

Search filters for quickly
building queries

Replace long-running
reports with live widgets



Opening Up the VM Detections Platform

Custom Remote Detections

Qualys Remote Detection
Interface (QRDI)

Create your own or share on
Qualys Community

Supports HTTP(S) and raw TCP

Regex grouping and capturing

LUA scripting for advanced logic

```
{} IPcam_QRDI.json •
1  {
2    "detection_type": "http dialog", "api_version": 1, "trigger_type": "dialog"
3    [
4      {
5        "transaction": "http get",
6        "object": "/cgi-bin/CGIProxy.fcgi?usr=visitor&pwd=testingqr",
7        "on_error": "stop"
8      },
9      {
10        "transaction": "process",
11        "mode": "regexp",
12        "match": "<firmwareVer>(.*)</firmwareVer>",
13        "extract": [{"var": "wholeMatch"}, {"var": "firmwareVersion"}]
14      },
15      {
16        "transaction": "report", "result": {"concat": ["Foscam Firm", "ware Version: ", "$firmwareVersion"]}
17      }
18    ]
19  }
20 }
```

Demo

Elastic VM Dashboard





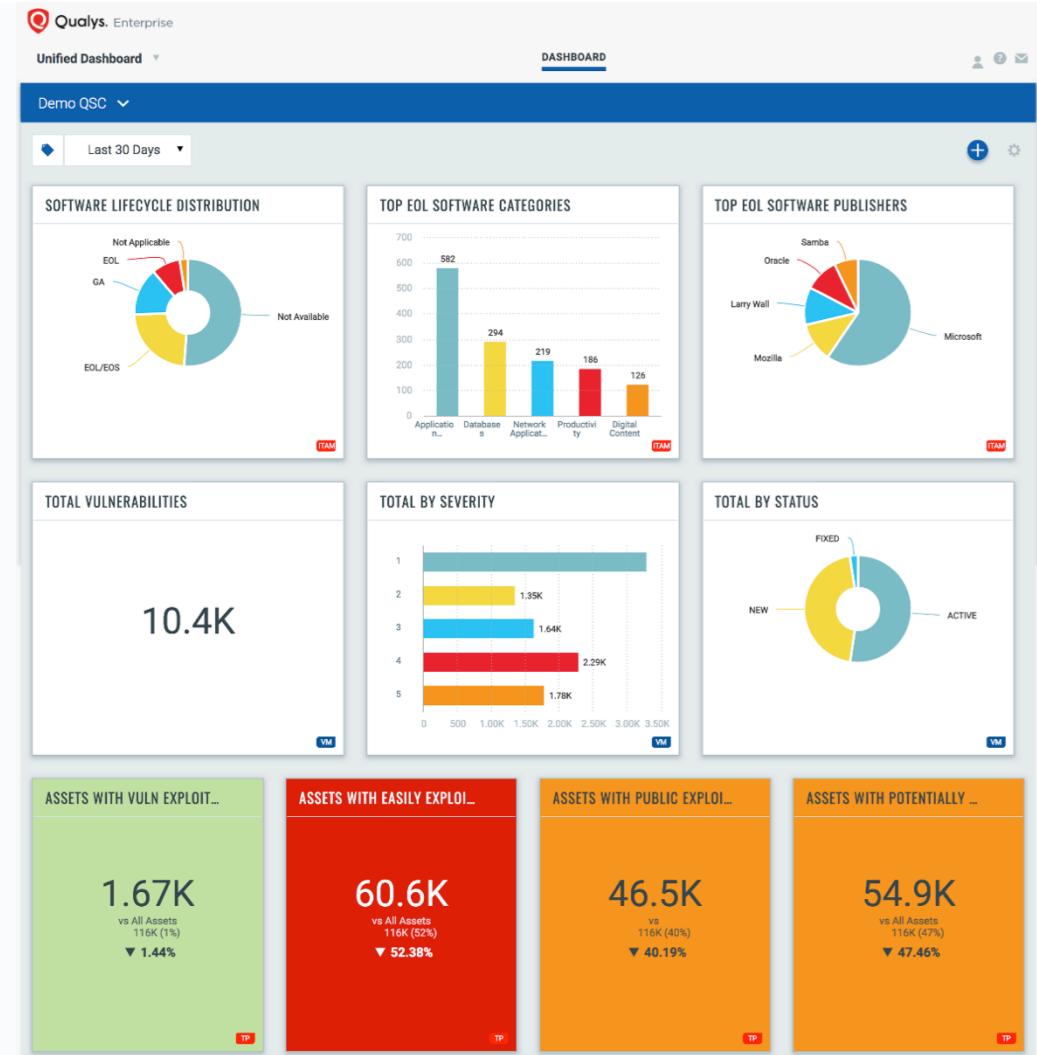
Unified Dashboards

Overview

Unified Dashboard

Build dashboards with widgets from multiple Qualys Cloud Apps

Target servers, containers, instances, web apps, etc. using Asset Tags



Demo



Unified Dashboard Preview

Microsoft .NET Framework Security Update (APSB11-CRITICAL-04)	MS17-NET-04	2017-05-22T11:00Z	APP	Windows	177113	CVE-2016-3127	No	2
Microsoft .NET Framework Security Update April 2017	APSB11-CRITICAL-04	2017-04-11T11:00Z	OS	Windows	197040	CVE-2016-0009	Yes	2
Microsoft SQL Server 2008 R2 Service Pack 3 (KB2979597)	MS17-NET-04	2017-05-22T11:00Z	APP	Windows	351175	CVE-2017-0477	Yes	1
Microsoft Windows Security Update May 2017	MS17-NET-04	2017-05-22T11:00Z	OS	Windows	197034	None	Yes	2
Oracle Java SE Critical Patch Update - April 2017	MS17-NET-04	2017-04-11T11:00Z	APP	Windows	170582	CVE-2016-6794	No	2
Security Update for Windows Server 2008 R2 SP4 Edition	MS16-NET-02	2016-07-12T11:00Z	APP	Windows	170582	CVE-2016-6794	No	2

Unified Dashboard Rollout

Phase 1

Unified Dashboard App
Global dashboard filters

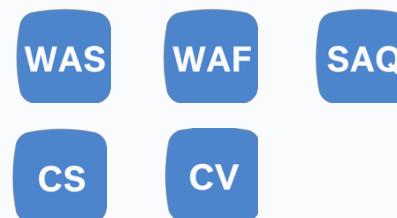
Support for:



Phase 2

Unified widget builder
Upgrade existing Cloud App Dashboards

Support for:

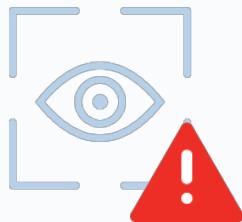


Qualys Patch Management

Overview

Current Patch Management Tools

Challenges and Impact



Manual correlation of vulnerability to patch leads to delayed mean-time-to-remediation

Waiting for vulnerability reports to confirm the patch has fixed the vulnerability

Remote systems only patched when connected to corporate network

Limited or no coverage of third-party apps

Multiple patching solutions for each OS type

Introducing Qualys Patch Management



The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.

Automated correlation of vulnerability and patch data
- Which patch fixes the CVE?

Simple dashboarding for tracking patch deployments

Patch using the Qualys Cloud Agent, anywhere

Patch OS and third-party applications

Single solution for Windows, macOS, and Linux



Shift From Reaction Mode to Operational Security



Always up-to-date on
missing patches

Security and IT teams can
“speak the same language”

Collaboration –key to
successful digital
transformation

Unify discovery, prioritization,
and remediation into one
platform

Rapid remediation of high-
profile vulnerabilities in days
vs. weeks

Regularly scheduled
deployments are repeatable
and reported on

Demo



Patch Management

Beta

Platform Support



XP SP3+
Vista
Windows 7
Windows 8/8.1
Windows 10
Server 2003 SP2+
Server 2008/R2
Server 2012/R2
Server 2016



OS X 10.10
Yosemite
OS X 10.11
El Capitan
macOS 10.12
Sierra
macOS 10.13
High Sierra
macOS 10.14
Mojave



RHEL 6,7
CentOS 5.4+,6,7
SUSE Linux
Enterprise Server/
Desktop 11,12,15
Oracle Ent Linux
6,7(Server)
Ubuntu 14.x,15.x,16.x,
18.x

- * Beta will focus on Windows- other operating systems will follow later
- * Roadmap items are future-looking; timing and specifications may change

Roadmap

Beta: Q4 2018 – Windows patch deployment

General Availability: Early 2019

Beta 1

Windows patching
(desktops and servers)

Qualys serves patches

Third party Windows
applications



Beta 2

On-prem Caching of
patches (QGS)

Direct download from
vendors for off-prem

Additional tokens for
dashboarding



Upcoming

Mac patching

Linux patching

Repository integration

Automation Rules &
Approval workflows



QUALYS SECURITY CONFERENCE 2018

Thank You

Michael Kassim
mkassim@qualys.com

Giorgio Gheri
ggheri@qualys.com